ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

ІІ ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ “ІННОВАЦІЙНІ ПІДХОДИ ДО РОЗВИТКУ ТЕХНОЛОГІЙ ТА ЕКОНОМІКИ”

ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Innovation and science

ЗАКАРПАТСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗУНУ

Свалява - 2025

ЗМІСТ

ФІШИНГ: НЕВИДИМА ЗАГРОЗА ЦИФРОВОГО СВІТУ

Хома Надія Григорівна,
кандидат фізико-математичних наук, доцент, доцент кафедри економічної кібернетики та інформатики,
Західноукраїнський національний університет,
khoma.nadiya@gmail.com,
Мушак Андрій Ярославович,
кандидат технічних наук, доцент, доцент кафедри економічної кібернетики та інформатики,
Західноукраїнський національний університет,
andriymushak1974@gmail.com

У сучасному світі, де онлайн-комунікація стала невід'ємною частиною нашого повсякденного життя, кіберзагрози постають перед нами дедалі частіше й у дедалі складніших формах. Однією з найпоширеніших та водночас найпідступніших загроз є фішинг– метод шахрайства, який базується не лише на технічних вміннях зловмисників, а й на використанні людських слабкостей, зокрема довіри, неуважності та нестачі цифрової обізнаності.

Суть фішингу полягає у спробі виманити конфіденційну інформацію під виглядом легітимної комунікації. Найчастіше зловмисники розсилають підроблені електронні листи, що нібито походять від банків, державних установ, відомих сервісів або популярних компаній. У таких повідомленнях користувачу повідомляють про термінову проблему – заблокований акаунт, підозрілу транзакцію, потребу підтвердити особистість або виграш у конкурсі. В листі зазвичай надається посилання, яке веде на фальшивий вебсайт, майстерно стилізований під справжній. Користувач, не підозрюючи нічого поганого, вводить свої логін, пароль або дані банківської картки – і ці дані одразу потрапляють до рук шахраїв [1].

Історія фішингу сягає ще 1990-х років, коли зловмисники почали використовувати підроблені сторінки America Online (AOL) для збору паролів. З того часу фішинг еволюціонував і сьогодні є частиною складної системи кіберзлочинності. Попри всі зусилля розробників захисних механізмів, ця форма шахрайства залишається актуальною, а іноді – навіть успішною через свою адаптивність і психологічну спрямованість [2].

Однією з причин ефективності фішингу є соціальна інженерія – сукупність методів впливу на поведінку людини задля досягнення потрібної реакції. Шахраї вміло імітують стиль офіційного листування, використовують справжні логотипи та навіть мову, притаманну певній організації. Листи часто оформлені без помилок, містять звертання на ім'я, а підпис – ідентичний підпису справжнього працівника компанії. Особливу увагу зловмисники приділяють створенню відчуття терміновості: мовляв, рахунок буде заблоковано через кілька годин, або користувач втратить доступ до даних,

якщо не вчинить відповідних дій. Такий психологічний тиск змушує людей діяти поспіхом, не аналізуючи ситуацію [3].

Фішинг також набуває нових форм. Крім електронної пошти, дедалі частіше застосовуються фішингові повідомлення у соціальних мережах, месенджерах і навіть SMS. Такі атаки отримали окремі назви: смішинг (від англ. SMS-phishing) і війшинг (від voice-phishing – телефонний фішинг). Наприклад, користувач може отримати SMS із повідомленням про вхід у банківський кабінет з незвичного пристрою. У повідомленні буде посилання на нібито офіційний сайт банку, де користувача попросять ввести свої дані. Або ж йому може зателефонувати псевдопредставник служби безпеки з попередженням про спробу зняття коштів і проханням надати код із SMS, що насправді є одноразовим паролем для переказу грошей.

Окрему загрозу становить так званий таргетований фішинг, або спірфішинг. У цьому випадку шахраї не розсилають масові листи, а навмисно обирають конкретну жертву – наприклад, бухгалтера компанії чи керівника відділу. Така атака ретельно планується: вивчається профіль особи в соціальних мережах, її посадові обов'язки, стиль спілкування. Потім надсилається персоналізований лист, який має на меті переконати отримувача виконати певну дію, наприклад, здійснити банківський переказ або надати доступ до внутрішньої системи. Через високий рівень деталізації такі атаки важко виявити навіть досвідченим користувачам.

Фішинг шкодить не лише окремим користувачам, а й організаціям. У випадку витоку корпоративної інформації можуть постраждати дані клієнтів, комерційні таємниці або інфраструктура компанії. У найгірших випадках фішинг може стати початком масштабної кібератаки, зокрема встановлення шкідливого програмного забезпечення, шифрування файлів та вимагання викупу. Саме тому багато компаній впроваджують спеціальні навчальні програми з кібербезпеки, які включають симуляції фішингових атак та інструктажі для співробітників.

Попри складність та витонченість сучасних фішингових методів, існують способи, які дозволяють знизити ризик стати жертвою. Одним із ключових елементів захисту є уважність. Варто звертати увагу на дрібні деталі: адресу відправника, спосіб звертання, граматичні помилки, підозрілі посилання. Надійні організації зазвичай не надсилають запити на введення паролів чи банківських даних через електронну пошту. Також не варто відкривати вкладення з листів, якщо їх походження викликає сумніви. Якщо виникає потреба перевірити інформацію, краще самостійно зайти на офіційний сайт або зателефонувати за номером, вказаним на офіційному ресурсі [4].

Іншим важливим аспектом є використання технічних засобів захисту. Це включає встановлення антивірусного програмного забезпечення, активацію двофакторної автентифікації, оновлення операційної системи та браузера. Сучасні веббраузери оснащені функціями розпізнавання фішингових сайтів, і

при спробі перейти за підозрілим посиланням можуть попередити користувача про можливу загрозу.

Нарешті, важливою є роль освіти. Розуміння того, як працює фішинг, та постійне оновлення знань у сфері цифрової безпеки дозволяє бути напоготові. Сьогодні знання про кібергігієну має бути не лише привілеєм IT-фахівців, а базовим навиком для кожного, хто користується електронною поштою, банкінгом або просто переглядає новини в інтернеті.

Світ фішингу динамічний, як і сам інтернет. Шахраї постійно вигадують нові схеми, адаптуються до технологічних змін і шукають найменші шпарини в нашій уважності. Але озброївшись знаннями, критичним мисленням і технічними засобами, ми можемо зробити себе менш вразливими до цієї загрози. У цифровому просторі, як і в реальному світі, обережність і обізнаність – найкращі засоби захисту [4].

Згадаймо приклади реальних кейсів фішингу, які демонструють масштаби та хитрість таких атак:

У 2016 році сталася одна з найгучніших фішингових атак, коли було зламано електронну пошту голови виборчого штабу Гілларі Клінтон – Джона Подести. Шахраї надіслали йому листа з повідомленням про підозрілу активність у його обліковому записі Google. Лист виглядав достовірно, і Подеста, за порадою помічників, натиснув на підроблене посилання й увів пароль. У результаті хакери отримали доступ до його переписки, яку згодом оприлюднили, вплинувши на хід президентських виборів у США.

Ще один відомий випадок – фішингова атака на компанію Facebook і Google, внаслідок якої вони втратили понад 100 мільйонів доларів. Зловмисник створив фальшиву компанію, яка видавала себе за одного з постачальників технічного обладнання, і надсилав підроблені рахунки на оплату. Обидві корпорації протягом кількох років переказували гроші на шахрайські рахунки, доки схему не було викрито.

У 2020 році під час пандемії COVID-19 зросла кількість фішингових атак, пов’язаних із темою коронавірусу. Зокрема, масово розсилалися електронні листи нібито від Всесвітньої організації охорони здоров’я з порадами щодо захисту від вірусу. Вкладені файли насправді містили шкідливе програмне забезпечення. Багато користувачів відкривали їх, не підозрюючи про обман, оскільки довіряли авторитету організації [5].

У 2021 році в Україні було зафіксовано низку фішингових атак під виглядом листів від "ПриватБанку". Користувачам приходили повідомлення про нібито заблоковані рахунки чи виграші у розіграші. Посилання вели на сайти, які імітували справжній інтерфейс банку. Після введення даних користувач втрачав доступ до свого облікового запису, а зловмисники отримували повний контроль над рахунком [6].

Ці кейси показують, що фішинг не має меж – ні географічних, ні технічних. Від нього страждають як пересічні користувачі, так і великі

корпорації. Єдиний дієвий спосіб протистояти – постійно підвищувати обізнаність і дотримуватися принципів цифрової безпеки.

Поширені ознаки фішингових листів і поясненням кожної наведено у наступній таблиці:

Ознака	Пояснення
Незвичайна адреса відправника	Лист нібито від банку, але email має дивний домен, наприклад @gmail.com
Помилки в тексті	Орфографічні або граматичні помилки, які не характерні для офіційних листів
Відчуття терміновості	Повідомлення на кшталт “Негайно підтвердьте” або “Ваш акаунт буде заблоковано”
Підозрілі посилання	Посилання, які на вигляд схожі на справжні, але ведуть на інший домен
Неочікувані вкладення	Файли, які користувач не чекав, часто з розширеннями .exe, .zip, .docm
Питання конфіденційної інформації	Запит на введення пароля, PIN-коду або даних картки – те, чого сервіси ніколи не роблять через email
Підроблений дизайн	Використано логотипи та форматування справжніх сайтів, але з незначними спотвореннями

Список використаних джерел:

1. Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.
2. Grimes, R. A. (2019). *Phishing attacks: Defending your organization from the silent threat*. Wiley.
3. Jakobsson, M., & Myers, S. (2007). *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft*. Wiley.
4. Кіберполіція України. (n.d.). *Офіційні попередження про фішинг*. Retrieved June 3, 2025, from https://cyberpolice.gov.ua
5. Anti-Phishing Working Group. (n.d.). *Phishing activity trends reports*. Retrieved June 3, 2025, from https://apwg.org
6. CERT-UA. (n.d.). *Національний координаційний центр кібербезпеки при РНБО України*. Retrieved June 3, 2025, from https://cert.gov.ua